The House Committee on Homeland Security's Subcommittee on Economic Security and Infrastructure Protection – "The Future of Cyber and Telecommunications Security at the Department of Homeland Security

September 13, 2006

William F. Pelgrin
Director
New York State Office of Cyber Security and
Critical Infrastructure Coordination

And

Chair of the
Multi-State Information Sharing and Analysis Center

Good Afternoon Chairman Lungren, Ranking Member Sanchez, and distinguished Members of the Subcommittee on Economic Security, Infrastructure Protection, and Cyber Security. I am William Pelgrin, the Director of New York State Office of Cyber Security and Critical Infrastructure Coordination and Chair of the Multi-State Information Sharing and Analysis Center (Multi-State ISAC).

I am honored to represent New York State and the Multi-State ISAC to discuss the challenges, successes and lessons learned in our efforts to address cyber security.

It is time for plain speaking—we must be open to sharing information. We must learn from the past to improve the future. Cyber security must be everyone's responsibility. I have adopted this mantra as a call to action.

Two days ago, we commemorated the 5th anniversary of the tragic events of September 11. Since 2001, much has been implemented to improve our nation's security posture. I am very proud of what has been accomplished in cyber security at both the New York State and Multi-State levels to assist in this effort to be more vigilant, prepared and resilient. But we cannot be complacent; we still have a long way to go.

Why We Must Be So Concerned?

- Cyber terrorism or human error can both have devastating consequences;
- Cyber attacks can originate from anywhere;
- The technology to launch such cyber attacks is relatively inexpensive and widely available; and
- Sophisticated computer expertise is no longer necessary to launch attacks.

My testimony today will describe our approach to address these issues and how we are working to improve the cyber security posture not only of New York State but of all the states and local governments in our nation. This could not have been done without the strong leadership of Governor Pataki, who has been a true champion of these issues.

Since it is the start that stops most of us, we took the approach of "let's just get started" using the "build it as you go" and "best effort" rules to move forward as quickly as possible.

The time to talk is over – it is the time for action.

For many it is very difficult to fully grasp the cyber challenges and threats that we face today. My method is to make it real and tangible in order to provide clarity and understanding of these issues.

None of us is as smart as all of us. Therefore, collaboration, cooperation and communication are the cornerstones of our approach. We can't do this alone. Our partnership with U.S. Department of Homeland Security has been a positive example of what can be accomplished when we truly work together toward a common goal.

Cyber security is more about management than technology. The best technology in the world, if not managed properly, with appropriate policies and procedures, will leave us vulnerable. We all must become champions for good cyber security practices and set an example for others to follow.

I would like to start off by describing my philosophy. I believe these guiding principles are major factors for our successes in New York, as well as with the Multi-State.

- First and foremost, it is not about one person or entity; it is about the collective effort.
- It is about moving in a common direction.
- Trust must be earned; it is not a right. We work hard to earn that trust.
- We have a willingness to share as much as possible without concern for what would or would not be shared with us. Over time, sharing is becoming two-way.
- The culture must change. Implementing sound cyber security practices must be as second nature as buckling a seatbelt.
- We continually strive to eliminate traditional bureaucratic impediments.
- We have created a safe haven in order to facilitate true collaboration and sharing.

The remainder of this testimony will describe how we addressed our challenges.

First, we needed to strategically realign our focus to meet the emerging threats.

Creation of the New York State Office of Cyber Security and Critical Infrastructure Coordination

The New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) was established in September 2002 by Governor George E. Pataki in order to have an entity with a single focus dedicated to addressing the highly specialized needs of cyber security and critical infrastructure coordination.

The Office is responsible for leading and coordinating New York State's efforts regarding cyber readiness and resilience; expanding the capabilities of the State's cyber incident response team; monitoring the State's networks for malicious cyber activities; coordinating the process by which State critical infrastructure data is collected and maintained; as well as leading and coordinating geographic information technologies.

Second, we focused on developing strong collaboration with the private sector.

NYS Public/Private Sector Cyber Security Workgroup

Because more than 85% of critical infrastructure is owned or controlled by the private sector, we immediately saw the need to create true partnerships. New York State actively engaged the private sector in addressing the State's cyber security and critical infrastructure needs.

Our NYS Public/Private Sector Cyber Security Workgroup comprises private sector high-level executives and public sector commissioners to represent critical industry sectors, including telecommunications, financial and economic, utilities, public safety, chemical, health, food and education/awareness. For example, for the Telecommunications Sector, we have as co-chair from the private sector, the Vice President and Chief Cyber Security Officer for AT& T, and for the public sector, the Chair of the NYS Public Service Commission.

The Workgroup is examining the current state of cyber readiness throughout the entities within each sector, working to identify and assess vulnerabilities and identify mitigation strategies.

The Workgroup has published two reports: *Cyber Security: Protecting New York State's Critical Infrastructure* details the on-going efforts in New York State to address cyber security readiness and response, in both the public and the private sectors; and The *Best Practice Guidelines for Cyber Security Awareness* which includes a number of useful tips and practical advice, along with links to additional information for all New Yorkers on how to become more "cyber security aware."

The Workgroup has expanded its participation to include all major entities within the sectors. These entities work closely with the established sector chairs and New York State to more fully engage those critical entities to share information and build important communication relationships.

The Workgroup meets monthly via conference call with each sector and meets together as a full group in person periodically. The participation in this Workgroup has been tremendous, and the information sharing relationship with the private sector serves to better prepare and protect New York State. This mutual information sharing arrangement is an important component in helping to ensure the readiness and resilience of New York State's critical infrastructure assets—both public and private. We are truly breaking down the traditional barriers that have prevented the public and private sectors from communicating. This Workgroup is important not only to New York, but the nation as well.

We are also working collaboratively on the national level with the private sector, through the National ISAC Council. The Council represents the critical industry sectors and focuses on advancing the physical and cyber security of the critical infrastructures of North America. I'm honored to have been elected to serve as Vice Chair of the ISAC Council. This is another great example of strong relationships between the public and private sectors.

Third, we recognized that traditional geographic borders are irrelevant when dealing with cyber security issues, so the need was clear for strong partnerships with other states and local governments across the nation.

Multi-State Information Sharing and Analysis Center (Multi-State ISAC)
The Multi-State ISAC is a voluntary and collaborative organization. I am pleased to say that we have 50 states and the District of Columbia as members, and we are actively pursuing local governments and territories. The mission of the Multi-State ISAC, consistent with the objectives of the *National Strategy to Secure Cyberspace*, is to provide a common mechanism for raising the level of cyber security readiness and response in each state and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the states and providing two-way sharing of information between and among the states and with local government.

The U.S. Department of Homeland Security has officially recognized the Multi-State ISAC as the national ISAC for the states and local governments to help coordinate cyber readiness and response.

Major Objectives of the Multi-State ISAC

- to provide two-way sharing of information on cyber critical infrastructure incidents and threats
- to provide a process for gathering and disseminating information on cyber and physical threats to cyber critical infrastructures
- to share security incident information among critical industry sectors
- to focus on the cyber and physical vigilance, readiness, and resilience of our country's cyber critical infrastructure assets
- to promote awareness of the interdependencies between cyber and physical critical infrastructure as well as between and among the different sectors
- to ensure that all necessary parties are vested partners in this effort

- to work collaboratively with the public and private sectors to foster communication and coordination
- to coordinate training and awareness

The following major initiatives reflect the successes we've accomplished at both the New York State level and the Multi-State ISAC level.

7x 24 Cyber Security Center

One of the key components in addressing our cyber security needs is the establishment of a 7x24 cyber security center. This Center provides cyber security monitoring for and analysis of intrusions and other anomalous cyber activity for New York State agencies and public universities, as well as the members of the Multi-State ISAC. The State has deployed Intrusion Detection/Prevention Systems (IDS/IPS) for the State agencies. Since the inception of the IDS/IPS program in May 2003, more than 17 billion log entries have been analyzed. Currently we also provide intrusion prevention monitoring for the State of Alaska, and several other states are actively engaging the MS-ISAC in considering similar arrangements.

The Center monitors cyber intelligence activity at a State, national and global level. It works closely with US-CERT, cyber researchers, security vendors and ISPs. The Center distributes cyber security advisories and alerts to all New York State agencies, to members of the private sector through its Public/Private Sector Workgroup and to other States and local governments through the Multi-State ISAC. New York State also posts cyber alerts and advisories on its public website: www.cscic.state.ny.us, and the Multi-State ISAC through its public website: www.msisac.org.

The Center monitors State and local government websites for web page defacements and affected entities are notified. In 2005, 1,169 defacements have been reported out to state and local governments.

Incident Response Team

New York State has an incident response team to respond to cyber incidents. A mandatory incident policy has been issued to all state agencies, which outlines what must be reported and how. The goal of this policy is to ensure that a state entity recovers from an incident in a timely and secure manner and to minimize impact. Reporting incidents to a central group promotes collaboration and information sharing with other sites that may be experiencing similar problems.

The Multi-State ISAC Members also report incidents to the Multi-State ISAC. The Multi-State ISAC serves as the liaison between the states and US CERT for cyber incident reporting.

Multi-State ISAC Secure Portal and Cyber Security Alert Map

The Multi-State ISAC uses the US-CERT portal as its secure portal. The Multi-State ISAC's compartment on this portal serves as a central repository for Multi-State ISAC members to utilize as a secure mechanism in sharing important, secure and vital information among the states. The portal allows for secure emailing and includes a library so that Multi-State ISAC members can readily share information and documents, such as statewide policies, procedures, and white papers.

One of the most unique features on the Multi-State ISAC secure portal is an alert map application that the Multi-State ISAC developed. This is a map of the nation, in which each state displays its current cyber security alert level, along with contact information for the Multi-ISAC Members. The Multi-State ISAC members have adopted this common Cyber Alert Indicator Protocol process; thus, when any Multi-State ISAC member state is at a "Guarded" level for cyber, for example, all of the other Multi-State ISAC Members will know the specific criteria used to arrive at that level.

State ISACs on the Secure Portal
A major step in fostering the strong relationships between and among state and local governments is the build-out of the secure portal so that each MS-ISAC Member state will have its own section of the portal in which to communicate securely, share documents, and display alert level status. This pilot is currently underway with five states.

These individual state "ISACs" will include representatives from state agencies, counties, cities and other municipalities and educational institutions and will provide the following benefits to members:

- direct access to cyber security threat information from the State
- access to security awareness materials, including computer-based training modules
- access to security policy templates
- access to security-related solutions
- periodic meetings, teleconferences and webcasts to promote peer networking and information sharing

This initiative is focusing on building strong relationships between and among the state and local government entities to best ensure our cyber readiness.

To view examples of the alert map and the individual state ISAC sections of the portal, please refer to Appendix A.

Local Government Committee
Local governments face the same cyber security issues. However, many of them can be at a disadvantage in addressing the issues due to lack of resources and

expertise. We are cognizant of the need for local government involvement and want local government as vested partners as we move forward.

To that end, I've established a Local Government Cyber Security Committee (Committee), with representatives from towns, counties, cities, and schools and state government. The Committee, established in May 2005, has been meeting monthly to develop a roadmap for addressing the cyber security needs of local governments. The Committee is focused on ascertaining the issues, building communication channels, and identifying mitigation strategies.

The Committee's goal was to develop a document that provides a non-technical resource to executives and managers to help them better understand the importance of cyber security and what they need to know about the issues.

The Committee has produced one of its first priority projects: the *Local Government Information Security: Getting Started* Guide. This is a brief, practical reference intended for entities that may not have the technology or information security expertise of other entities and therefore need a basic "how to get started" resource for addressing information security challenges.

This Guide is a joint effort with the U.S. Department of Homeland Security's National Cyber Security Division.

The *Getting Started* guide covers the following topics:

- Introduction to Information Security
- Why is Information Security Important
- What is an Unprotected Computer
- What is a Cyber Incident
- Top Ten Things that must be done
- Glossary of information security terms
- Daily/weekly/monthly/annual checklist for the designated information security individual(s)

Future volumes of the Guide will include appendices that expand on the topics presented in the first volume, providing more detail about the steps necessary to secure the information which the citizens have entrusted to local governments. The appendices will be distributed in installments periodically over the year and will contain non-technical, plain language descriptions with specific action steps, along with references for further information.

We are also working on compiling a national database of contact information for local government representatives so that we can communicate more effectively and share information, including cyber alerts and advisories, future appendices of the Guides and other relevant information.

National Webcast Initiative

The MS-ISAC, in cooperation with the U.S Department of Homeland Security, through its National Cyber Security Division, has launched a partnership to deliver a series of national webcasts which examine critical and timely cyber security issues.

Embracing the concept that "cyber security is everyone's responsibility," these webcasts are available to a broad audience to help raise awareness and knowledge levels. The webcasts provide practical information and advice that users can apply immediately. All sessions are recorded and archived for viewing via the MS-ISAC public website.

Thousands of individuals from across the country and around the world participate in the webcasts.

One of the highlights of the webcast program is the national webcast held in October as part of National Cyber Security Awareness Month. This webcast is focused on how to keep our children safe online and features an interactive play for 4th and 5th grade age levels. The session will be broadcast live via the Internet and satellite and will be rebroadcast several times throughout the day to maximize viewing in each time zone. Last October, more than 5,000 teachers, parents, students and others participated in that broadcast and we look forward to another successful event this October 4!

To view a listing of all webcasts conducted through the National Webcast Initiative, please refer to Appendix B.

Partnership with U.S. Department of Homeland Security, National Cyber Security Division

As highlighted in this testimony, the Multi-State ISAC has a strong partnership with the National Cyber Security Division (NCSD) and its operational arm, the US-CERT. Through this partnership, we work together on many initiatives including sharing and analyzing information regarding cyber threats and events, conducting national webcasts, publishing cyber security awareness materials, conducting cyber exercises, as well as National Cyber Security Awareness Month activities. These initiatives help further the goal of improving our nation's cyber security posture.

Training and Awareness Activities

In New York, we have a number of ongoing training and awareness activities including:

- *Annual Statewide Cyber Security Conference.* We just held our ninth annual Cyber Security Conference. This Conference is free of charge to government employees. Consistent with our motto that "Cyber Security is everyone's responsibility," the scope of the Conference has expanded over the years to where we now provide multiple tracks covering a wide spectrum of cyber security issues, including technical, legal, auditing, academia, business managers and local government. This is the largest free government conference of its type in the country.
- *Annual Kids Safe Online Conference*. We are sponsoring our second annual Kids Safe Online Conference next month. Our target audience includes parents, educators, law enforcement officers as well as kids. The subject is not only what are the dangers for children online, but what are the solutions. This Conference is free to the public.
- *Information Security Officers (ISOs).* New York was the first state to appoint a statewide Information Security Office and I believe the first to require each agency to appoint an information security officer. The agency ISOs have a dotted line reporting relationship with my Office. We hold monthly meetings with the ISOs where we focus on current issues and training opportunities. Agency ISOs are required to have twenty-four hours a year of continuing professional education. We also sponsor statewide cyber security training for ISOs and technical staff. For example, we are currently sponsoring a seven-week online course for information security professionals to increase their skills.
- *Technical Staff.* We are sponsoring training on secure coding for application developers. In the past, we provided a 12 week course designed to increase the cyber security knowledge of technical staff and prepare staff to sit for the CISSP (Certificated Information Security Systems Professional) Exam. This training was video taped and made available to state and local governments on a national level.
- *Senior Staff.* Once a year, we provide a half-day awareness session for agency heads and their senior staff. The focus is to keep them informed of cyber security issues and to ensure they have the requisite knowledge to address them. It's also important to employ unique and creative solutions to increase awareness and education. We need to make it real. One of the approaches I took was to demonstrate to agency commissioners what is really meant when a computer is hacked. By having them see first-hand what could happen, it increased their awareness of the importance of cyber security.
- *End Users.* We developed a toolkit for State agencies, along the same line as the toolkit developed for the Multi-State ISAC. This includes calendars, mouse pads and posters, all with the cyber security message. We also produced a cyber security video that is used for training new employees at State agencies, as well as local governments. This was also made available to state and local governments on a national level. In addition, we conducted a "phishing exercise" with several state agencies to assess

the current state of cyber awareness and identify where further education is necessary.

- *Cyber Exercises.* We sponsor and participate in periodic cyber security exercises to test our plans, policies, practices and procedures.

In our role as Coordinator of the Multi-State Information Sharing and Analysis Center, we work with states to develop, share and collaborate on training and awareness activities including:

- *Proclamations:* In 2005, thirty-six Multi-State ISAC members reported that proclamations were issued by their respective governors proclaiming October 2005 as Cyber Security Awareness month. This is an increase of twenty-four from the previous year. This demonstrates the increasing awareness of cyber security issues at the state level. A copy of our 2005 Cyber Security Month After-Action Report is attached.
- *Tool Kits.* We develop an annual tool kit for the states to use to promote Cyber Security Awareness. This includes posters, calendars, mouse pads and new for 2006 is the development of Public Service Announcements that are customized for each state.
- *Cyber Exercise.* In partnership with U.S. Department of Homeland Security, we coordinate Multi-State (state and local government) participation in regional and national exercises to test our plans, policies, practices and processes in responding to a cyber event. We need to insure that we have the capability to provide prompt and accurate situational awareness reports at the state and national level.
- *Technical Training.* We coordinate state participation of state and local governments in national training programs sponsored by the federal government. We also negotiate some volume discounts for states to participate in training provided by the private sector.
- *End User.* We are just completing the development of a Computer Based Training Program that will be made available to state and local governments nationally. This is a tutorial which educates end users on the basics of information security and what their responsibilities are to safeguard our government information systems. We publish a monthly Cyber Security Newsletter for end users. The newsletter focuses on one cyber security issue each month that is relevant for end users/home users. The newsletter is distributed to the states and local government which then push it out to the end users.

For a summary of the MS-ISAC Accomplishments, please refer to Appendix C.

Funding for the Multi-State ISAC

We very much appreciate the fiscal support from the Department of Homeland Security for the Multi-State ISAC. The current funding level of one million dollars a year amounts to twenty thousand dollars per state. While we have worked hard to leverage this available funding, more meaningful, long lasting change would be possible if more funding was available. Our ability to help raise the awareness and preparedness of states and local governments (for example, intrusion prevention monitoring and correlation of data) to help improve their cyber security posture is constrained due to the limited fiscal resources.

I appreciate the opportunity to testify today. Thank you Chairman Lungren and Members of this Subcommittee for your strong leadership and attention to this important matter.